NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 8705.2A
Effective Date: February 07, 2005
Expiration Date: February 07, 2010

Printable Format (PDF)

Subject: Human-Rating Requirements for Space Systems

Responsible Office: Office of Safety and Mission Assurance

Appendix B. Definitions

B.1 Abort: Termination of the nominal mission that allows the crew and passengers to be returned to Earth in the portion of the space system used for nominal entry and touchdown.

B.2 Automated: Automatic (as opposed to human) control of a system or operation.

B.3 Autonomous: Ability of a space system to perform operations independent from ground control and other space systems. This includes no communication with, or real-time support from, the ground control or other systems.

B.4 Breakout: During proximity operations, the ability to maneuver one or more vehicles to a safe separation distance.

B.5 Certification: Certification is documentation that validates that the requirements were correct, the system will perform its mission in the expected environment, and verifies that the requirements were met.

B.6 Crew: Any human on board the space system while in flight that has been trained to interact with the space system; same as flight crew.

B.7 Crew and Passengers: Every human on the space flight vehicle.

B.8 Crew Escape: See definition for escape.

B.9 Crew Survival: Capability and ability to preclude crew fatality or permanent disability.

B.10 Critical Functions: Capabilities or functions that are essential to the safety of the crew and passengers, that if lost would cause loss of life or permanent disability.

B.11 Critical Software: Any software component whose failure or unanticipated performance could lead to the loss of the flight crew and passengers or space system. This includes the flight software as well as ground-control software that can affect flight safety.

B.12 Critical System: A system is assessed as critical if loss of overall system function, or improper performance of a system function, could result in loss of life, loss of vehicle, or damage to the system.

B.13 Design for Minimum Risk: A process in which risks are reduced through specified margins of safety, factors of safety, material properties, or any other properties inherent to the design of the part, component, subassembly, or assembly. The process includes design implementation and verification provisions to enhance the safety critical reliability of space systems to the maximum extent practical.

B.14 Deviation: A written authorization for a variance where the requirement will not be met, but through an alternate means, the system will have an equivalent or lower lever of risk.

B.15 Escape: Removal of crew and passengers from the portion of the space system normally used for reentry, due to rapidly deteriorating and hazardous conditions, thus placing them in a safe situation suitable for survivable return or recovery. Escape includes, but is not limited to, those modes that utilize a portion of the original space system for the removal (e.g., pods, modules, or fore bodies).

B.16 Exception: A written authorization given to the program, allowing the program relief from, or an alternative to, a requirement, because that requirement does not apply to any of the subsystems.

B.17 Fail-Safe: Ability to sustain a failure and retain the capability to safely terminate or control the operation.

B.18 Fault: A defect, imperfection, mistake, or flaw of varying severity that occurs within some hardware or software component or system. "Fault" is a general term and can range from a minor defect to a failure.

B.19 Flight Crew: Any human on board the space system while in flight that has been trained to interact with the space system; same as crew.

B.20 Hazard: Existing or potential condition that can result in or contribute to a mishap.

B.21 Human Error: Either an action that is not intended or desired by the human or a failure on the part of the human to perform a prescribed action within specified limits of accuracy, sequence, or time that fails to produce the expected result and has led or has the potential to lead to an unwanted consequence.

B.22 Human Health Management and Care: The set of activities, procedures, and systems that provide (1) environmental monitoring and human health assessment; (2) health maintenance and countermeasures; and (3) medical intervention for the diagnosis and treatment of injury and illness.

B.23 Human Performance: The physical and mental activity required of the crew and other participants to accomplish mission goals. This includes the interaction with equipment, computers, procedures, training material, the environment, and other humans.

B.24 Human-Rated Space System: A space system that incorporates those design features, operational procedures, and requirements necessary to accommodate human participants such that:

a. Risks have been evaluated and either eliminated or reduced to acceptable levels;

b. Human performance and health management and care have been appropriately addressed such that the system has been certified to safely support human activities; and

c. The capability to safely conduct human-tended operations has been provided, including safe recovery from any credible emergency situation.

B.25 Human-Rating Board: The following group of NASA senior management that performs executive level activities for the Human-Rating Requirements: Chief Engineer, Chief Health and Medical Officer, Chief Safety and Mission Assurance Officer, Associate Administrator for Space Operations, and Associate Administrator for Exploration Systems.

B.26 Human-Rating Certification: Human-rating certification is the documented authorization granted by the Associate Administrator for Space Operations that validates that the system will perform its mission in the expected environment, and verifies with objective quality evidence that the requirements were met allowing the program manager to operate the space system within its prescribed parameters for its defined reference missions. Human-rating certification is obtained prior to the first crewed flight (for flight vehicles) or operational use (for other systems).

B.27 Human-Rating Independent Review Team: An independent group of technical experts who reviews program products during the human-rating certification process and provides recommendations to NASA Headquarters senior management.

B.28 Human-Rating Plan: A formal document detailing the human-rating requirements that will be applied to a specific space system from System Requirements Review to system disposal at end of life. The Human-Rating Plan provides traceability from NPR 8705.2, Human-Rating Requirements for Space Systems, and includes rationale for all tailoring and exceptions. The Human-Rating Plan includes a verification matrix for all human-rating requirements that indicates how the requirements in the plan will be met, and the specific objective quality evidence that will be used to verify or demonstrate compliance with each requirement.

B.29 Human-Rating Process: The process steps used to achieve a human-rated space system. These steps include human safety risk identification, reduction, control, visibility, and program management acceptance criteria. Acceptable methods to assess the risk to human safety include qualitative and/or quantitative methods such as hazards analysis, fault tree analysis, human error analysis, probabilistic risk assessment, and failure modes and effects analysis.

B.30 Intervention Capability: The ability of the crew to assert control over all space system functions in nominal and off-nominal situations.

B.31 Manual Control: The crew's ability to bypass automation in order to exert direct control over a space system or operation.

B.32 Objective Quality Evidence: Any statement of fact, either quantitative or qualitative, pertaining to the quality

of a product or service based on observations, measurements, or tests which can be verified. (Evidence will be expressed in terms of specific quality requirements or characteristics. These characteristics are identified in drawings, specifications, and other documents which describe the item, process, or procedure.)

B.33 Office of Primary Responsibility: The Office that is designated as "Responsible Office" for the requirements document.

B.34 Override: To take precedence over system control functions.

B.35 Passenger: Any human on board the space system while in flight that has no functional responsibility to perform any mission task for that system.

B.36 Permanent Disability: Any occupational injury or illness that does not result in a fatality or permanent total disability, but, in the opinion of competent medical authority, results in permanent impairment through loss of or compromised use of any part of the body, with the following exceptions: loss of fingernails or toenails, loss of tip of fingers or tip of toe without bone involvement, inguinal hernia (if it is repaired), or sprains or strains that do not cause permanent limitation of motion. Any nonfatal injury or occupational illness that, in the opinion of competent medical authority, permanently and totally incapacitates a person to the extent that he or she cannot follow any gainful occupation and results in a medical discharge or civilian equivalent.

B.37 Proximity Operations: Two or more vehicles operating near enough to each other so as to have the potential to affect each other. This includes rendezvous and docking (including hatch opening), undocking, and separation (including hatch closing).

B.38 Public: All humans not participating in the space flight activity who could be potentially affected by the function or malfunction of the space system.

B.39 Reliability: The probability that a system of hardware, software, and human elements will function as intended over a specified period of time under specified environmental conditions.

B.40 Rescue: The process of locating the crew, proceeding to their position, providing assistance, and transporting them to a location free from danger.

B.41 Risk: The combination of (1) the probability (qualitative or quantitative) including associated uncertainty that the space system will experience an undesired event (or sequences of events) such as internal system or component failure or an external event and (2) the magnitude of the consequences (personnel, public, mission impacts) and associated uncertainties given that the undesired event(s) occur(s).

B.42 Risk Assessment: An evaluation of a risk item that determines (1) what can go wrong, (2) how likely is it to occur, and (3) what the consequences are.

B.43 Safe Haven: A functional association of capabilities and environments that is initiated and activated in the event of a potentially life-threatening anomaly and allows human survival until rescue or repair can be affected.

B.44 Safety: The freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

B.45 Space System: Any system developed and/or operated that supports activity in space, including, but not limited to, subsystems supporting launch, mission control, and operations.

B.46 Supportability: The degree of ease to which system design characteristics and planned logistic resources, including the logistics support elements, allow for the meeting of system availability and operational utilization requirements.

B.47 Tailoring: A process where a written authorization is given to the program from the Independent Technical Authority or designees prior to the approval of the Human-Rating Plan, allowing the program to exclude or modify a requirement in NPR 8705.2, Human-Rating Requirements for Space Systems, from the Human-Rating Plan, because the system does not have the component/subsystem described in that requirement, and consequently the requirement does not apply as written. For example, the system is not a flight vehicle; therefore it is not required to perform flight tests.

B.48 Test Flight: A flight occurring prior to certification.

B.49 Usability Testing: Evaluation by people using the system (hardware or software) in a realistic situation to determine how well it can be used for its intended purpose (e.g., how well people can manipulate parts or controls, receive feedback, and interpret feedback) to identify potential human errors and areas for design improvement.

B.50 Validation: (1) An evaluation technique to support or corroborate requirements to ensure that necessary functions are complete and traceable; or (2) the process of evaluating software at the end of the software development process to ensure compliance with software requirements.

B.51 Variance: Documented and approved permission to perform or avoid some act or operation contrary to

established requirements. A variance is an exception, deviation, or waiver.

B.52 Verification: The process of proving or demonstrating that requirements have been satisfactorily met through design and/or operational elements.

B.53 Verification Plan: A formal document listing the specific technical process to be used to show compliance with each requirement.

B.54 Waiver: A written authorization allowing a variance from a specific requirement where there is an increase in risk. The waiver includes a formal acceptance of risk by the program manager and by an official authorized to speak for the risk-takers when they do not fall under the authority of the program.

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | AppendixA | AppendixB | AppendixC | ALL |

| NODIS Library | Program Management(8000s) | Search |

DISTRIBUTION:
NODIS